Application No.: 09/726,822
Amendment Dated: March 8, 2006
Reply to Office Action of: September 8, 2005

IN THE CLAIMS:

Please amend the claims as indicated. A complete set of the claims is included below, reflecting added subject matter *(underlining)* and deleted subject matter *(strikethrough)*, as well as the current status of each claim. This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method for preventing unauthorized transfer of data between a portable computer system and systems of data storage and communication including another computer, said method comprising:

a) automatically receiving identification authentication information for said portable computer system at a communication interface device embodied as a cradle for said portable computer system, wherein said authentication information comprises a unique identity for said portable computer system and wherein said authentication information is embedded in said portable computer system;

b) comparing at said communication interface device said identification authentication information with a list of authorized portable computer system identities;

c) determining at said communication interface device whether said portable computer system identity is authorized based on said identification authentication information and said unique identity;

d) enabling at said communication interface device communication between said portable computer system and said other computer provided said identity is authorized and disabling said communication if said identity is not authorized; and

e) enabling at said communication interface device decryption of encrypted data from said portable computer system provided said identity is authorized and disabling decryption if said identity is not authorized.

2. (Canceled)

Application No.: 09/726,822
Amendment Dated: March 8, 2006
Reply to Office Action of: September 8, 2005

3. (Previously Presented) The method as recited in Claim 1, wherein said identification authentication information is transferred from said portable computer system to said interface device to uniquely identify said portable computer system to said interface device.

4. (Canceled)

5. (Canceled)

6. (Previously Presented) The method as recited in Claim 1 wherein said b) comprises:

recognizing said identification authentication information as an indication of unique identity of the source sending said information; and

indexing said unique identity to a list of programmed identities.

7. (Previously Presented) The method as recited in Claim 1 wherein said c) comprises:

reacting to positive indexing match as an authenticated authorized identity and to negative indexing match as an unauthorized identity; and

authorizing communications enablement in response to an authenticated authorized identity, and prohibiting communications in response to an unauthorized identity.

8. (Previously Presented) The method as recited in Claim 1 wherein said d) comprises:

allowing said portable computer to synchronize with said other computer upon authorization of communication; and

preventing synchronization upon prohibition of communication.

9. (Previously Presented) The method as recited in Claim 1 wherein said e) comprises:

disclosing a specific key value with which said data is encrypted upon authorization of communication; and

not disclosing said specific key value upon prohibition of communication.

10. (Currently Amended) A system for preventing unauthorized transfer of data between a portable computer system and a host system, comprising:

a) a portable computer device capable of synchronizing with said host;

b) an interface device compatible to receive said portable computer device and capable of facilitating communication between said portable computer device and said host system;

c) an identification authenticating component ~~incorporated~~ embedded into one of said devices and providing a unique identification signal corresponding to the unique identity thereof; and

d) an identification authorizing component capable of determining if said unique identity is authorized for synchronization and for correspondingly enabling and disabling synchronization between said portable computer and said host system, wherein decryption of encrypted data from said portable computer device is enabled provided said unique identity is authorized and wherein said decryption is disabled if said unique identity is not authorized.

11. (Previously Presented) A system as recited in Claim 10 wherein said portable computer device comprises a palmtop computer.

12. (Previously Presented) A system as recited in Claim 10 wherein said interface device comprises a palmtop computer cradle.

13. (Previously Presented) A system as recited in Claim 10 wherein said synchronous communication is further encrypted with a specific key value from said identification authenticating tagging component such that unauthorized applications external to said portable computer system are locked out from deciphering data therefrom.

Application No.: 09/726,822
Amendment Dated: March 8, 2006
Reply to Office Action of: September 8, 2005

14. (Previously Presented) A system as recited in Claim 10 wherein said identification authenticating tagging component is a magnetic key and said identification authentication reading component is a magnetic key reader.

15. (Previously Presented) A system as recited in Claim 10 wherein said identification authenticating tagging component is a smart card and said identification authentication reading component comprises a smart card reader.

16. (Previously Presented) A system as recited in Claim 10 wherein said identification authorizing component comprises is an application specific integrated circuit.

17. (Previously Presented) A system as recited in Claim 10 wherein said identification authorizing component comprises a software program.

18. (Previously Presented) A system as recited in Claim 10 wherein said identification authenticating tagging component is in direct electrical connection with said identification authentication reading component via contacts.

19. (Previously Presented) A system as recited in Claim 10 wherein said identification authenticating tagging component is in contact free communication with said identification authentication reading component via an infrared communication mechanism.

20. (Previously Presented) A system as recited in Claim 10 wherein said identification authenticating tagging component is in contact free communication with said identification authentication reading component via a transmitter/receiver modality and antenna array.

21. (Currently Amended) A system for preventing unauthorized transfer of data between a portable computer system and a system of data storage and communication, comprising:

a) a portable computer device capable of synchronizing with said system of data storage and communication;

b) an interface device compatible to receive said portable computer device and coupled with said system of data storage and communication and capable of facilitating communication between said portable computer device and said system of data storage and communication;

c) an identification authenticating tagging and data encryption keying component ~~incorporated~~ embedded into one of said devices and providing a unique identification signal and an encryption key cipher value corresponding to the unique identity thereof;

d) an identification authentication reading component capable of sensing and reading said unique identification signal incorporated into the other of said devices not incorporating said tagging component;

e) an identification authorizing component receiving input from said reading component and incorporated into the same one of said devices as said reading component, capable of determining if said unique identity is authorized for synchronization and of correspondingly enabling and disabling synchronization between said portable computer and said system of data storage and communication; and

f) an identification authorizing component further capable of enabling deciphering of encrypted communication from said portable computer device if said unique identity is authorized and disabling decryption if said unique identity is unauthorized.

22. (Previously Presented) A system as recited in Claim 21 wherein said identification authorizing component incorporates software for determining if said unique identity is authorized for synchronization, for correspondingly enabling and disabling synchronization, and deciphering encrypted data from said portable computer device.

23. (Currently Amended) A communication system comprising:

a host computer system comprising a communication port;

Application No.: 09/726,822
Amendment Dated: March 8, 2006
Reply to Office Action of: September 8, 2005

a portable electronic device comprising a communication port and an identity reference, said identity reference embedded into said portable electronic device; and

a communication interface module separate from said host computer system for coupling between said communication ports of said portable electronic device and said host computer system, said communication interface module comprising:

an authentication device for authenticating said identity reference; and

a communication interface circuit coupled to said authentication device and for allowing direct communication between said portable electronic device and said host computer system provided said authentication device indicates a proper authentication of said identity reference and, otherwise, for disallowing communication between said portable electronic device and said host computer system, wherein decryption of encrypted data from said portable computer device is enabled provided said unique identity is authorized and wherein said decryption is disabled if said unique identity is not authorized.

24. (Previously Presented) A communication system as recited in Claim 23 wherein said communication interface circuit comprises a decryption circuit.

25. (Previously Presented) A communication system as recited in Claim 23 wherein said communication module contains a slot for receiving said communication port of said electronic device.

26. (Previously Presented) A communication system as recited in Claim 23 wherein said identity reference is stored on a removable smart card.

27. (Previously Presented) A system as recited in Claim 21 wherein said interface device is a palmtop computer cradle.

28. (Previously Presented) A system as recited in Claim 23 wherein said communication module is a palmtop computer cradle.